

# إلى ةدنتسمل م دختسمل ةقداصم نيوكت TACACS و RADIUS

## تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسمل تانوكملا](#)

[نيوكتلا](#)

[مكحتلا تادحوو vEdge ل لي وختلا او RADIUS إلى ةدنتسمل م دختسمل ةقداصم](#)

[مكحتلا تادحوو vEdge ل TACACS ل ع نيوميأقلا صيوفتلا او م دختسمل ةقداصم](#)

[قلاص تاذا تاملولعم](#)

## ةمدقملا

radius ل TACACS إلى ةدنتسمل م دختسمل ةقداصم نيوكت ةيفيكي دنتسمل اذه حضوي ISE م دختسمل مكحتلا تادحوو vEdge.

## ةيساسألا تابلطتملا

### تابلطتملا

دنتسمل اذهل ةصاخ تابلطتم دجوت ال

### ةمدختسمل تانوكملا

يتلا مكحتلا تادحوو vEdge-cloud ISE. نم 2.6 رادصلإ م ادختسإ م تي، ةيحصإ إلى ضارغلل 19.2.1 رادصلال لغشت

ةصاخ ةي لمعم ةئيبي في ةدوجوملا ةزهجال نم دنتسمل اذه في ةدراول تاملولعملا عاشنإ م تناك اذإ. (يضا رتفا) حوسمم نيوكتب دنتسمل اذه في ةمدختسمل ةزهجال عيمج تادب رمأ يال لمحتحمل ريثأتلل كمهف نم دكأتف، ليغشتلا دي قكتكبش

## نيوكتلا

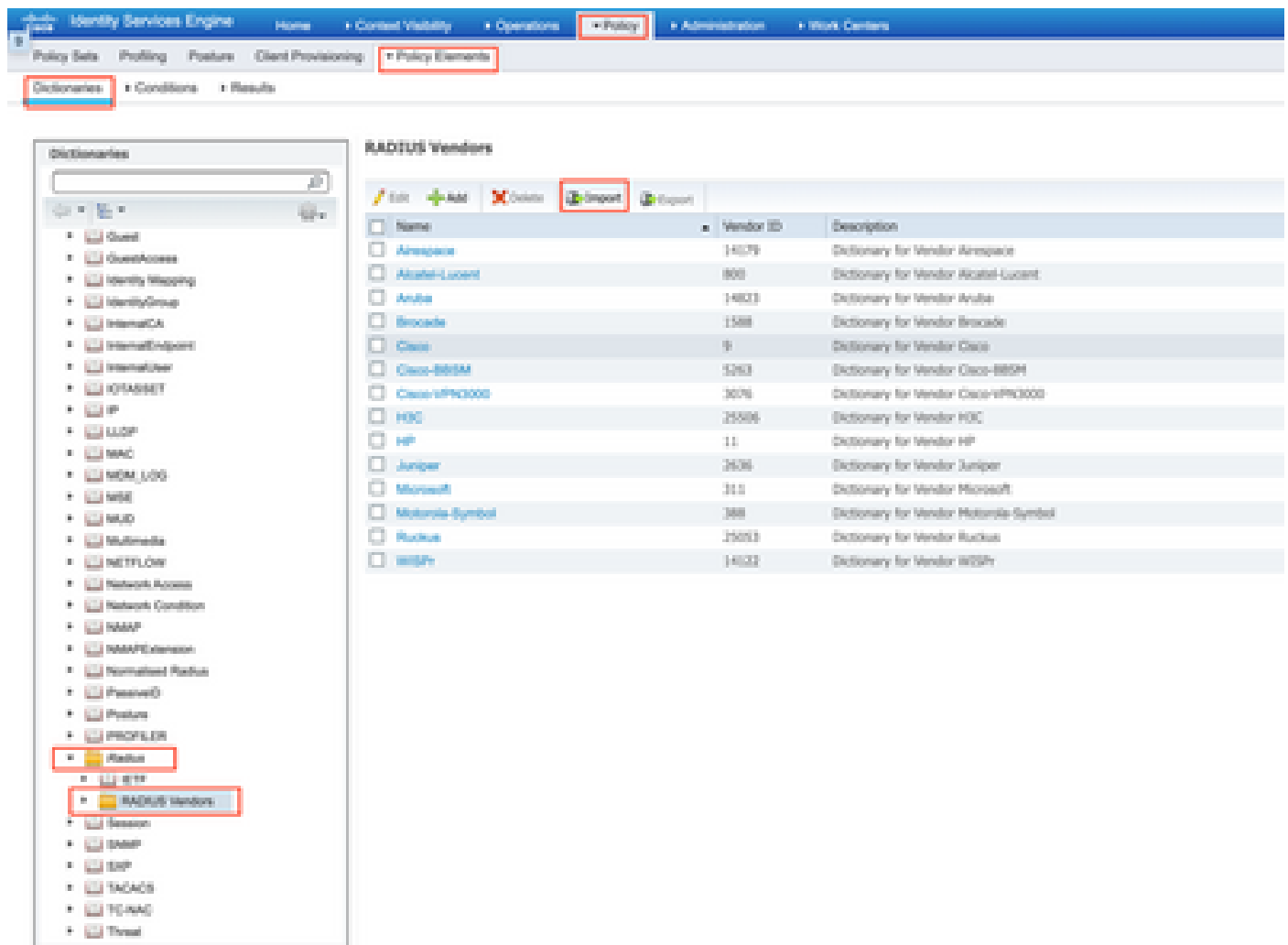
ةتباثل ني م دختسمل تاعومحمل عامسأ ةثالث Viptela جم انرب رفوي م دختسمل عضو م تي. لقالا ل ع ةدحو و عومحمل م دختسمل نيبيعت ب جي. operator. ةيساسألا ةومحمل في ايئاقلت يضا رتفال TACACS/RADIUS.

مكحتلا تادحوو vEdge ل لي وختلا او RADIUS إلى ةدنتسمل م دختسمل ةقداصم

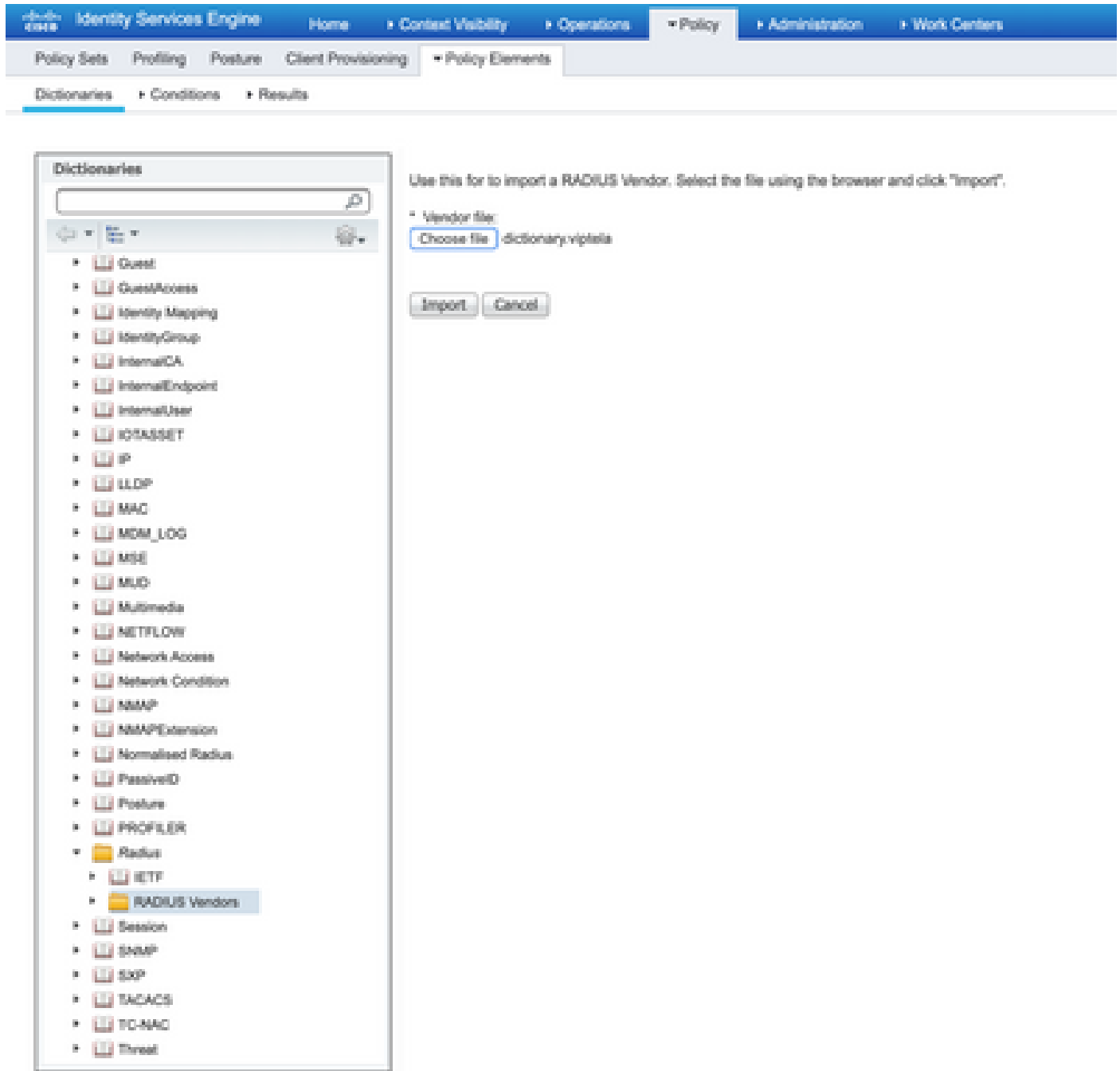
يصرن فلم ءاشنإب مق ،كلذب مايق لل . ISE ل Viptela radius سوماق ءاشنإب مق 1. ةوطخلل  
 ىوتحملل اب:

```
# -*- text -*-
#
# dictionary.viptela
#
#
# Version:      $Id$
#
VENDOR          Viptela          41916
BEGIN-VENDOR    Viptela
ATTRIBUTE       Viptela-Group-Name 1 string
```

> ةسايسلل رصانع > ةسايسلل ىلل لقتنا ،ضرغلا اذهل . ISE ىلل سوماقلا لىمحت 2. ةوطخلل  
 وه امك داريتسإ رقتنا مث RADIUS ىدروم > Radius ىلل لقتنا ،سىماوقلا ةمئاق نم . سىماوقلا  
 حضم.

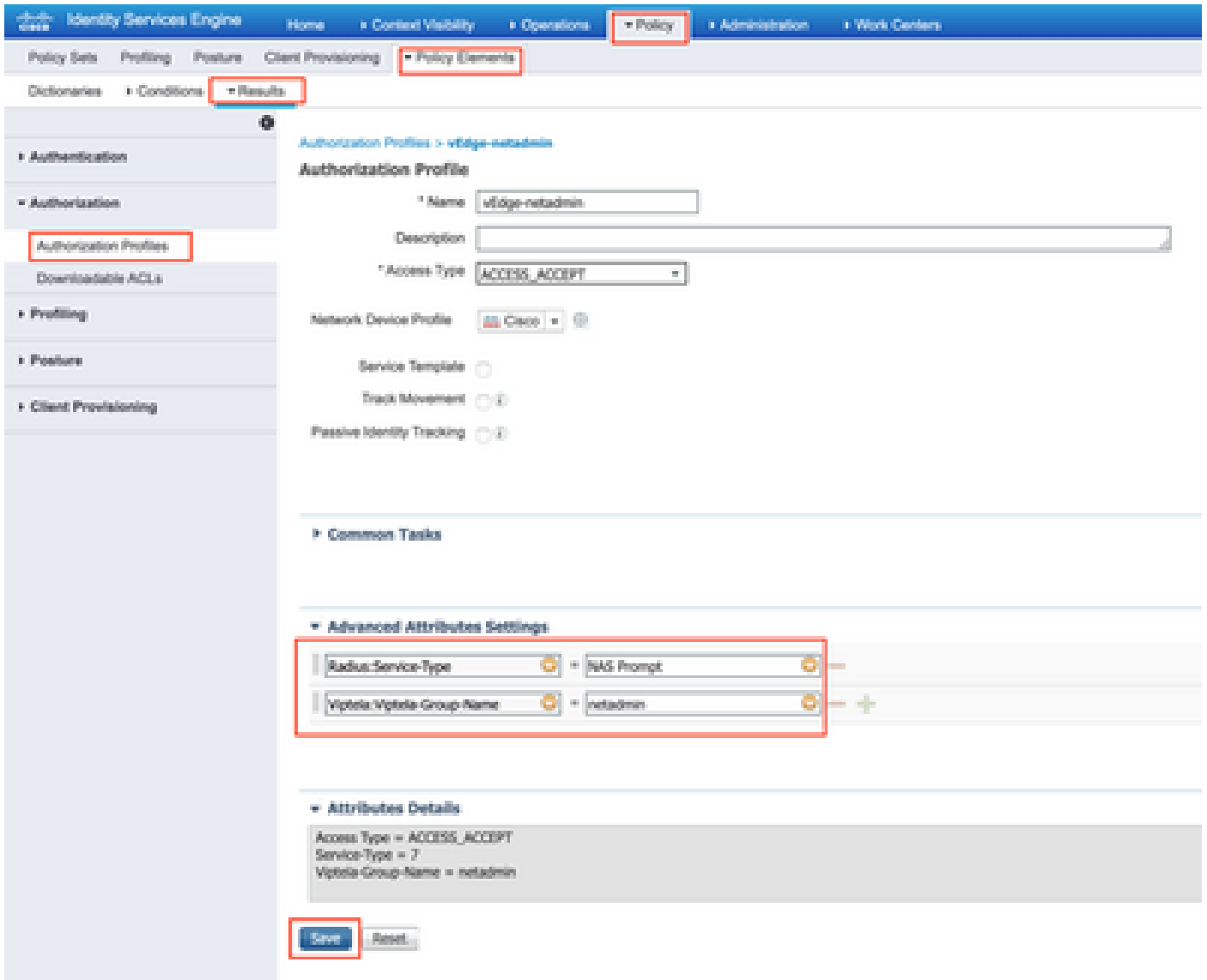


## 1. ةوطخلال ي ف هتأشنأ يذلا فلملا لي محتب مق

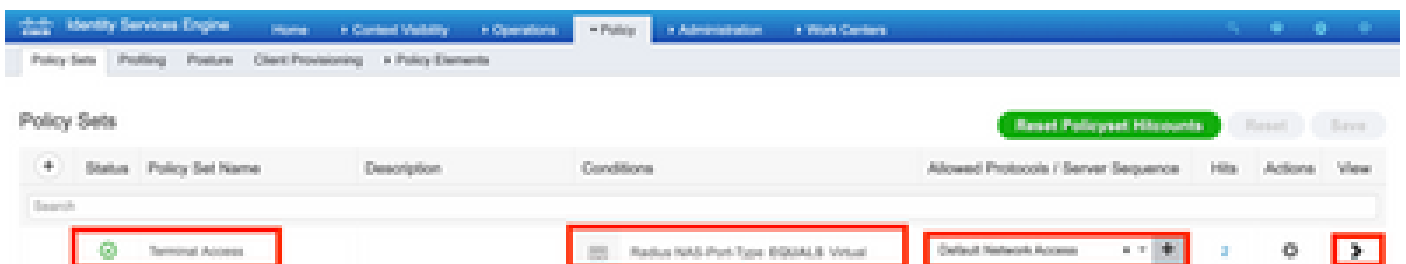


The screenshot shows the Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' tab is active, and the 'Policy Elements' sub-tab is selected. The 'Dictionaries' section is open, showing a list of dictionaries. The 'RADIUS Vendors' folder is expanded, and the 'dictionary.viptela' file is selected. A dialog box is open for importing a RADIUS vendor file. The dialog box contains a search bar, a list of vendor files, and buttons for 'Import' and 'Cancel'.

RADIUS، ةوطخلال هذو ي ف . ليوخت فيرعت فلم ءاشنإ 3. ةوطخلال لقتنا، اذهل . هيلع قدصم مدختسمل NetAdmin زايتما يوتسم نييعتب، لاثملا ليلبس يلع نيتمدقتم نييتي صاخ دحو ليوختلا صي صخت تافلما > ةسايسلا رصانع > ةسايس يلإ ةروصلال ي ف حضوم وه امك .



ضارغأل .كب صخال ليلع فال دادعإل لاقف و فلتخم لكشب جهنلا ةعومجم و دبت دق 4 ةوطخل لوصول ىمسي يذلا ةسايسلا لاخذإ ءاشنإ متي ، ةلاقمل هذه يف يحيضوتل ضرعل ةروصل يف حضوم وه امك يف رطلال .



ةروصلال يف حضوم وه امك ةيلال ءاشنلا رهظتو > رقنا .

Identity Services Engine | Home | Config | Visibility | Operations | Policy | Administration | Work Centers

Policy Sets | Profiling | Posture | Client Provisioning | Policy Elements

Policy Sets → Terminal Access Reset Policyset Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
<span>+</span>	Terminal Access		Radius NAS-Port-Type ISDNALB Virtual	Default Network Access	
<span>+</span>	Authentication Policy (1)				
<span>+</span>	Authorization Policy - Local Exceptions				
<span>+</span>	Authorization Policy - Global Exceptions				
<span>-</span>	Authorization Policy (2)				

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
<span>+</span>	vEdge-remote	IdentityGroup Name ISDNALB User Identity Group:lab_admin	vEdge-remote	Select from list	1	<span>⚙️</span>
<span>+</span>	Default		CompAccess	Select from list		<span>⚙️</span>

Reset Save

فلم ني عي و lab\_admin ني مدخست ملة و عوم جم في رعت فلم يلى اذانت سا جهنلا اذ قباطتي  
 3. ةوطخلال ي هؤاشن مت لي وخت في رعت

ةروصلال ي ف حضوم وه امك (vEdge مكحت ةدحو و هجوم) NAS في رعت ب مق 5. ةوطخلال

Identity Services Engine Administration

Network Resources

Network Devices List > vEdge-01

**Network Devices**

\* Name: vEdge-01

Description: [ ]

IP Address: [ 10.48.87.232 / 32 ]

\* Device Profile: Cisco

Model Name: [ ]

Software Version: [ ]

\* Network Device Group

Location: All Locations [ Set To Default ]

IPSEC: No [ Set To Default ]

Device Type: All Device Types [ Set To Default ]

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

\* Shared Secret: [ \*\*\*\*\* ] [ Show ]

Use Second Shared Secret:  [ i ]

CoA Port: 1700 [ Set To Default ]

RADIUS DTLS Settings [ i ]

DTLS Required:  [ i ]

Shared Secret: radius/dtls [ i ]

CoA Port: 2083 [ Set To Default ]

Issuer CA of ISE Certificates for CoA: Select if required (optional) [ i ]

DNS Name: [ ]

General Settings

Enable KeyWrap:  [ i ]

\* Key Encryption Key: [ ] [ Show ]

\* Message Authenticator Code Key: [ ] [ Show ]

Key Input Format:  ASCII  HEXADECIMAL

مكتمل إعداد حو vEdge نيوك ت 6 ة و ط خ ل ا

```

system
aaa
auth-order radius local
radius
server 10.48.87.210
vpn 512
key cisco
exit
!
!

```

NetAdmin ةومجم نبيعت نم دكأتو vEdge لى لودل ليجستب مق. قحتل 7. ةوطخل ديعل مدختسملل

```
vEdgeCloud1# show users
```

SESSION	USER	CONTEXT	FROM	PROTO	AUTH GROUP	LOGIN TIME
33472	ekhabaro	cli	10.149.4.155	ssh	netadmin	2020-03-09T18:39:40+00:00

تادحوو vEdge ل TACACS لى نع نيمئاقلا ضيوفتلاو مدختسملل ةقداصم مكحتل

TACACS فيرت فلن نبيعت متي، ةوطخل هذه في TACACS فيرت فلن ءاشن 1. ةوطخلل هتقداصم تمت مدختسمل NetAdmin زايتما يوتسم، لاثملا لىبس لىع، هؤاشن متي ذل

- كةمسلا ةفاضلا ةصصخملا ةمسلا مسق نم يمازلإ دح:

ةمقلا	مسالا	عونلا
Netadmin	Viptela ويديفلا ةومجم مسالا	يمازلإ

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > **Device Settings**

Network Access > Guest Access > TrustSec > EPOD > Profiles > Posture > **Device Administration** > Password

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > **Policy Elements** > Device Admin Policy Sets > Reports > Settings

TACACS Profiles > vEdge

TACACS Profile

Name: vEdge\_netadmin

Description: [Empty]

Task Attribute View | Rule View

Common Tasks

Common Task Type: [Shell]

Default Privilege: [ ] (Select 0 to 15)  
 Maximum Privilege: [ ] (Select 0 to 15)  
 Access Control List: [ ]  
 Auto Comment: [ ]  
 No Escape: [ ] (Select true or false)  
 Timeout: [ ] Minutes (0-9999)  
 Idle Time: [ ] Minutes (0-9999)

Custom Attributes

+ Add | Trash | Edit

Type	Name	Value
Mandatory	Violate-Group-Name	netadmin

Cancel | Save

2. قوطخل SD-WAN ل زهجا ةومجم عاشنإ.

Identity Services Engine

Home > Context Visibility > Operations > Policy > **Administration** > Work Centers

System > Identity Management > **Network Resources** > Device Profile Management > uGSM Services > Post Service > Threat Center NAC

Network Devices > **Network Device Groups** > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > External NEM > Location Services

Network Device Groups

All Groups | Choose group

Network | Add | Edit | Show group members | Import | Export | Pin Table | Expand All | Collapse All

Name	Description	No. of Network Devices
All Device Types	All Device Types	-
<b>Blindfish</b>		5
All Locations	All Locations	-
All IPSEC Device	With a RADIUS user IPSEC Device	-



## Add Group



Name

Description

Parent Group

Cancel

Save

SD-WAN: إعدادة ومجموعة إلى هني عت و زاهج ل ني وكت ب مق 3. ووطخل

Network Devices List > vEdge-01

### Network Devices

Name

Description

IP Address  /

Device Profile

Model Name

Software Version

### Network Device Group

Location

IPSEC

Device Type

### TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

### SNMP Settings

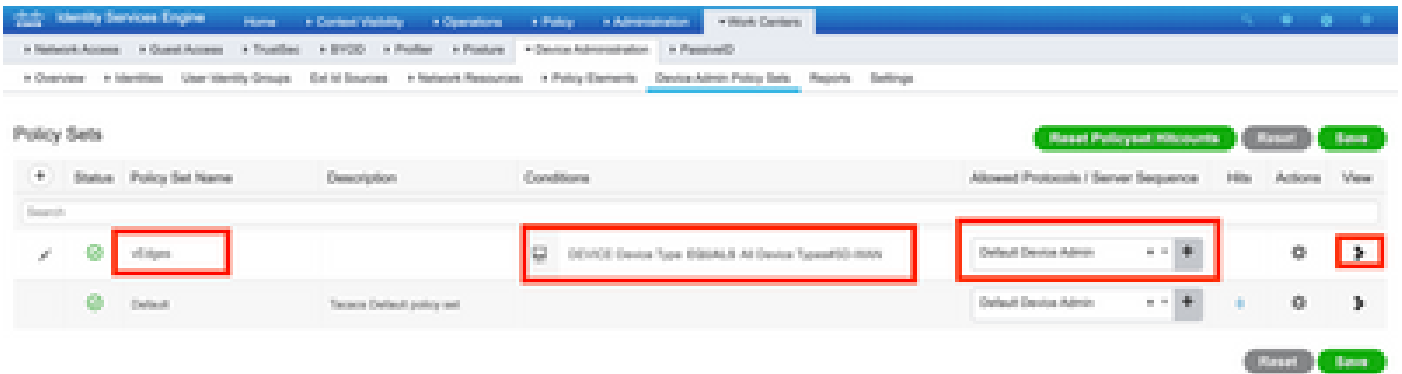
### Advanced Truflow Settings

Save

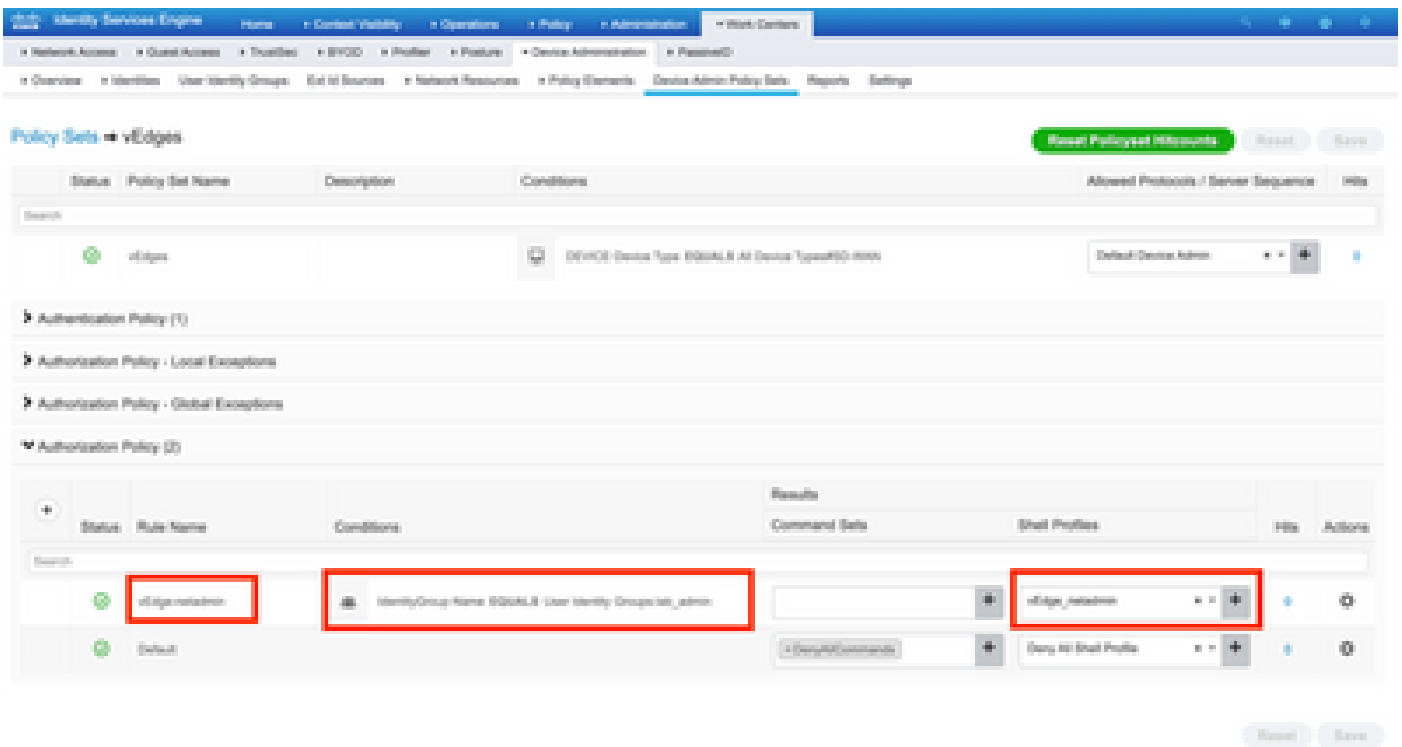
Reset

إعدادة أ ل ق راد ا ه ن دي دحت 4. ووطخل

ضرع ال ضارغل .كب صاخل ال يلعل ال دادع ال لاقف و فل تخم لك شب جهن ال ة عومجم و دبت دق ة سايس ال ءاشنإ متي ،دنت سمال اذف يف يحضو ال



عم جهن ال اذف قباطتي . ةروصل ال هذه يف حضوم وه امك ة ي ال ال ة شاش ال رهظتو > قوف رقنا ة و طخل ال يف هؤاشنإ متي يذل Shell فيرعت فلم ني عي و SD-WAN ي سمال زا هال عون 1.



vEdge ني وكت 5. ة و طخل ال

```

system
aaa
  auth-order tacacs local
!
tacacs
  server 10.48.87.210
  vpn 512
  key cisco
exit
!
!

```

ةوعومجم نييغت نم دكأتو vEdge جم انرب يلى لوخدلا ليحستب مق .ققحتلا 6. ةوطخلا  
ديعبلا مدختسملل NetAdmin

```
vEdgeCloud1# show users
```

SESSION	USER	CONTEXT	FROM	PROTO	AUTH GROUP	LOGIN TIME
33472	ekhabaro	cli	10.149.4.155	ssh	netadmin	2020-03-09T18:39:40+00:00

## ةلص تاذا تامولعم

- دةزه أةرادال يفي رعنتلا رشنلا ليلد Cisco ISE: <https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973>
- ةقداصل او مدختسملل لوصو نيوكت: [https://sdwan-docs.cisco.com/Product\\_Documentation/Software\\_Features/Release\\_18.4/02System\\_and\\_Interface](https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interface)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت  
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و  
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems ( ر ف و ت م ط ب ا ر ل ا ) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا